REMARKS

In the Office Action[1], the Examiner rejected claims 1-7, 9-15, 17-37, 39-45, 47-69, 71-73, 75-90, and 138-157 under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,949,877 to Traw et al. ("*Traw*").

By this amendment, Applicants amend claims 1, 4, 5, 7, 9, 11, 14, 17, 18, 21, 28-34, 36, 37, 39, 41, 44, 47, 48, 51, 58-64, 66, 68, 69, 73, 75, 76, 78, and 85-90, and cancel claims 3, 6, and 67 without prejudice or disclaimer. Applicants respectfully traverse the rejection under 35 U.S.C. § 102(b) for the reasons discussed below.

Independent claim 1, for example, recites a data transmitting system comprising, among other things, a "portable optical disc medium including ... a security module ...and an optical disc distinct from the security module." *Traw* fails to teach or suggest at least the claimed portable optical disc medium.

Traw discloses a method for protecting digital content from copying or other misuse when transferring the content between compliant devices over insecure links (*Traw*, abstract). *Traw's* method works by distributing a "Certificate Revocation List" (CRL) from a license authority to various devices (*Traw*, col. 5, lines 37-42). *Traw* discloses implementing the method in compliant devices such as "traditional consumer electronics products including but not limited to DVD player/recorders, digital televisions, set top boxes, digital satellite services receivers, and similar products" (*Traw*, col. 2, lines 51-60).

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement or characterization in the Office Action.

Traw, however, does not disclose distributing the CRL on a portable optical disc medium with a security module. Instead, *Traw* discloses using communications such as an IEEE 1394 bus between separate devices to distribute the CRL (*Traw*, col. 3, lines 25-34). While *Traw* discloses that other devices, such as disk drives, could be used to distribute the CRL, this passage of *Traw* merely contemplates using the disk drive itself, rather than a portable medium readable by the disk drive, to securely distribute the list (*Traw*, col. 3, lines 31-33). Although *Traw* discloses compliant media can also be used to distribute the CRL, *Traw* discloses doing so on media as manufactured (*Traw*, col. 6, lines 48-52) and not by incorporating a security module with the media.

Applicants pointed out these deficiencies in the Traw reference in a Reply to Office Action filed August 27, 2008. The Office Action responds by alleging that "the term 'portable data storage medium' is not limited to an optical disc or medium ... it could be interpreted to be any device that includes memory" (Office Action at p. 11). Applicants respectfully disagree that any device that includes a memory can constitute a "portable data storage medium." Nevertheless, Applicants have amended the claims to recite a "portable optical disc medium." As Traw does not disclose an optical disc medium comprising a security module, Traw does not teach or suggest the claimed "portable optical disc medium including ... a security module ...and an optical disc distinct from the security module" as recited by independent claim 1.

Although of different scope, independent claims 34 and 64 distinguish over the four cited references for at least the same reasons as claim 1. Claims 2-7, 9-15, 17-33, and 138-145 depend from claim 1, claims 35-37, 39-45, 47-63, and 146-153 depend from claim 34, and claims 65-69, 71-73, 75-90, and 154-157 depend from claim 64.

Because the cited references fail to teach or suggest each and every element recited by claims 1-7, 9-15, 17-37, 39-45, 47-69, 71-73, 75-90, and 138-157, no *prima facie* case of obviousness has been established with respect to these claims. Applicants therefore request the Examiner to withdraw the rejection of these claims under 35 U.S.C. § 103(a).

The dependent claims are further distinguishable from *Traw*. Claim 10, for example, recites "[t]he system as set forth in Claim 1, wherein the security module stores a revocation list of illegal drive units." As discussed, *Traw* merely discloses exchanging a CRL between various consumer electronic devices. *Traw* does not disclose or suggest that the is stored in a security module of a portable optical disc medium. Instead, *Traw* contemplates that the CRL is exchanged when a user actively connects one device to another, such as using a 1394 interface (*Traw*, col. 3, lines 30-34). Thus, *Traw's* CRL is updated in a different manner than the revocation list of claim 10, because the revocation list of claim 10 is stored in a security module on a portable optical disc medium and thus can be securely updated when a new medium is installed in the drive unit.

Traw suffers from the deficiency that only complete devices are equipped to securely exchange the CRL. As discussed, while *Traw* discloses compliant media can also be used to distribute the CRL, *Traw* discloses doing so on media as manufactured (*Traw*, col. 6, lines 48-52) and not by incorporating a security module. Thus, when *Traw's* system distributes the CRL using media containing the CRL, noncompliant or revoked devices could simply read the CRL from the media due to the absence of a security module on the media itself. Accordingly, *Traw* fails to teach or suggest at least

"wherein the security module stores a revocation list of illegal drive units," as recited by independent claim 10.

Claim 24 recites a system "wherein the illegal unit revocation list includes ... a registration list identifying units that have not been revoked" (emphasis added). As discussed above, *Traw* discloses distributing a CRL. However, *Traw* merely discloses that the CRL includes "devices whose compliance has been revoked" (*Traw*, col. 3, lines 38-40) (emphasis added). *Traw* does not disclose a list identifying devices that have not been revoked. Therefore, *Traw* does not teach or suggest "wherein the illegal unit revocation list includes ... a registration list identifying units that have not been revoked," as recited by claim 24.

Claim 33 recites a system wherein "the security module reads data encrypted and stored in the portable optical disc medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit" (emphasis added). As discussed, while *Traw* discloses that compliant media can be used to distribute the CRL, *Traw* discloses doing so on media as manufactured (*Traw*, col. 6, lines 48-52). Conventional media lack a security module that can re-encrypt data read from the conventional media. Thus, *Traw's* media do not "decrypt" and "re-encrypt" any data using a security module. Therefore, *Traw* does not teach or suggest the claimed "security module reads data encrypted and stored in the portable optical disc medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit" (emphasis added), as recited by dependent claim 33.

In view of the foregoing remarks, Applicants respectfully request reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 27, 2009

By: /David W. Hill/
David W. Hill
Reg. No. 28,220